Cloud Service Contracts: An Issue of Trust

Marie Demoulin
Assistant Professor – Université de Montréal
École de Bibliothéconomie et des Sciences de l’Information (EBSI)
iTrust 2d International Symposium, Victoria, 16th Oct. 2014
Workgroup members

• **Researcher**
  – Marie Demoulin, Université de Montréal

• **Graduate research assistants**
  – Jessica Bushey, UBC
  – Robert McLelland, UBC
Research object

Contract
as a tool to build
Trust
in the Cloud
Research question

How effective are cloud service contracts at addressing the needs of records managers and archivists?
Milestones

- iTrust Project 10: Contract terms with cloud service providers
  - Cloud contracts vs RM’s needs
- iTrust Project 14: Trust in Cloud Service Contracts
  - Cloud contracts vs RM and archivists’ needs
  - Standards and Legal framework
- Also linked to Project 6: Retention and disposition in the cloud
Selected contracts

• Boilerplate contracts
  – No room for negociation – Take it or leave it
• Cloud Services relevant for RM and archivists
  – No consumer contracts
• Contractual (binding) documents
  – No marketing material
  – Terms of Service (ToS)
  – Service Level Agreement (SLA)
  – Privacy Policy, Acceptable Use Policy, Security Terms...
• Jurisdiction
  – Canada – US – Europe
Selected standards

- ISO 15489:2001 – Records management
- ISO 14721:2002 – Preservation of records
- ISO 14721:2012 – Open Archival Information System (OAIS)
- ARMA’s Recordkeeping Principles (2013)
- Moreq 2009
Legal framework

- Canada – US – EU
- Transverse view on
  - Freedom of information law (public bodies)
  - « Patriot » laws
  - Privacy law
  - Evidence law (esp. Civil law)
  - Ownership principles
Research Product

• Check-list for record managers and archivists to:
  – Understand boilerplate cloud contracts
  – verify if they meet their needs
  – clarify recordkeeping needs to legal and IT departments
  – communicate recordkeeping needs to cloud providers
Methodology

- Literature review and annotated bibliography
  - Legal, archival and RM literature on cloud contracts
  - Existing recommendations for private and public bodies
- Identify RM and archival needs & functions to be considered in the contract
- Clarify the legal framework linked to these needs
- Compare with a sample of cloud provider contracts
- Identify gaps
- Cloud contracts Reader’s Check-list
Cloud contracts Reader’s Check-list
(Preliminary results)

- Data ownership
- Availability, retrieval and use
- Data retention and disposition
- Data storage and preservation
- Security, confidentiality and privacy
- Data location and cross-border data flows
- End of Service – Contract termination
Gaps

- Data retention and disposition
- Data preservation
- Data location
- End of contract

- Not (fully) addressed in the majority of the contract terms
Data Ownership

• Who owns
  – the data stored, transmitted or created in the cloud by the customer (i.e. you)?
    • Does the service provider have the right to use them and, if so, to what extent?
  – the associated metadata generated by the system/provider?
    • Do you have the right to access to them for recordkeeping or legal purposes
      – during the contractual relationship?
      – at the end of the contract?
Availability, retrieval and use

- Precise indicators and providing clear information about the availability of the service?
- Does the degree of availability of the data fit with your business needs?
  - allow you to comply with
    - the freedom of information legislation (if public body),
    - the right of a person to access to her own personal data
    - the right of authorities to legally access to your data for investigation, control or judicial purposes?
Data retention and disposition

• Are your data (and all their copies) destroyed
  – In compliance with your data retention and disposition schedules
  – Immediately and permanently
  – According to a secure destruction policy?

• Associated metadata generated by the provider
  – Need to be destroyed? Same time & same manner?
  – Will the service provider proceed to such destruction?

• Audit trails?
  Attestation or report of deletion? (if requested)
Data storage and preservation

- Who is responsible for backups and for recovering the data?
- Are records migrated or emulated in a way that preserves their authenticity, reliability, integrity and usability?
  - Audit trails?
- How will the service evolve?
  - Will you be noticed of any evolution that could impede the authenticity of your data?
Security, Confidentiality & Privacy

- Does the system prevent unauthorized access, use, alteration or destruction of the data through technical, physical and organizational measures?
  - Audit trails, metadata and/or access logs to demonstrate this?
- Will you be noticed in the case of security breach or system malfunction?
- Any subcontractor?
  - Information about the identity of the subcontractor and its tasks?
- Confidentiality policy of the service provider, in regards to its employees, partners and subcontractors?
- Any special confidentiality or security policy for sensitive, confidential, personal or other special kinds of data?
- Is the service provider accredited and/or is he audited
  - on a systematic, regular and independent basis by a third-party in order to demonstrate that he complies with his security, confidentiality and privacy policies?
  - Is such a certification or audit process documented?
    - Certifying or audit body and expiration date of the certification?
Data location & Cross-border data flows

• Where is the location of the data (and their copies)?
  – Does it comply with the location requirements imposed by law? (if applicable)
  – Will you be notified if the data location is moved outside your jurisdiction?

• Does the contract mention the possibility of disclosure orders by national or foreign security authorities?
  – Will the provider inform you and ask for your consent prior to disclosure? (if allowed by law)
End of Service – Contract termination

• Duration of the contract?
  – Why and how can it be terminated?
  – Any prior notification?

• At the end of the contract, whatever the reason
  – Warranty that your data will be restored in a usable and interoperable format?
    • Time, procedure and cost?
    • Provider’s assistance?
  – Right to access to the associated metadata generated by the system?
  – After restitution of data, immediate and permanent destruction?
Next steps

• Consolidation of the results
  – From check-list to guidelines
    (vs. « model contract »)
• Collaboration with iTrust Project 6 – Retention and disposition in the cloud (Pat Franks)
  – Comments and suggestions are welcome:
    • Marie.demoulin@umontreal.ca
Dissemination

• *Canadian Journal of Information and Library Science*
  - Special Issue on Data, Records and Archives in the Cloud (June 2015)
  • Paper submitted (October 2014)